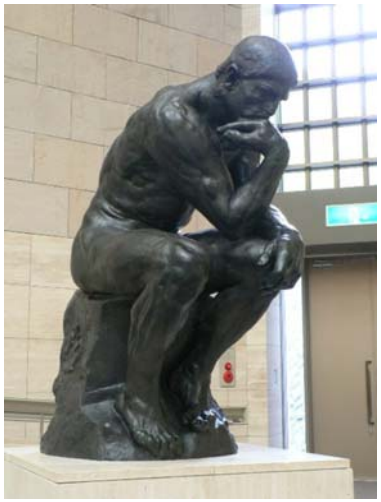
Androidが抱えるセキュリティ問題
～他分野への提言～

2010年10月20日
KDDI研究所　竹森敬祐



Confidential
©2010 KDDI R&D Laboratories Inc.
KDDI R&D LABS

他分野連携の必要性

- Androidの思想
  - Androidは、モバイル機能が付いたPCである。
  - セキュリティはユーザ責任である。
  - アプリケーションの開発と販売の自由化を図り、開発者とユーザを集める。

- 今後の予測
  - PCの利用経験のない世代まで、Android端末は普及する。

  ⇒ PCで発生していたインシデントが大規模に発生する。

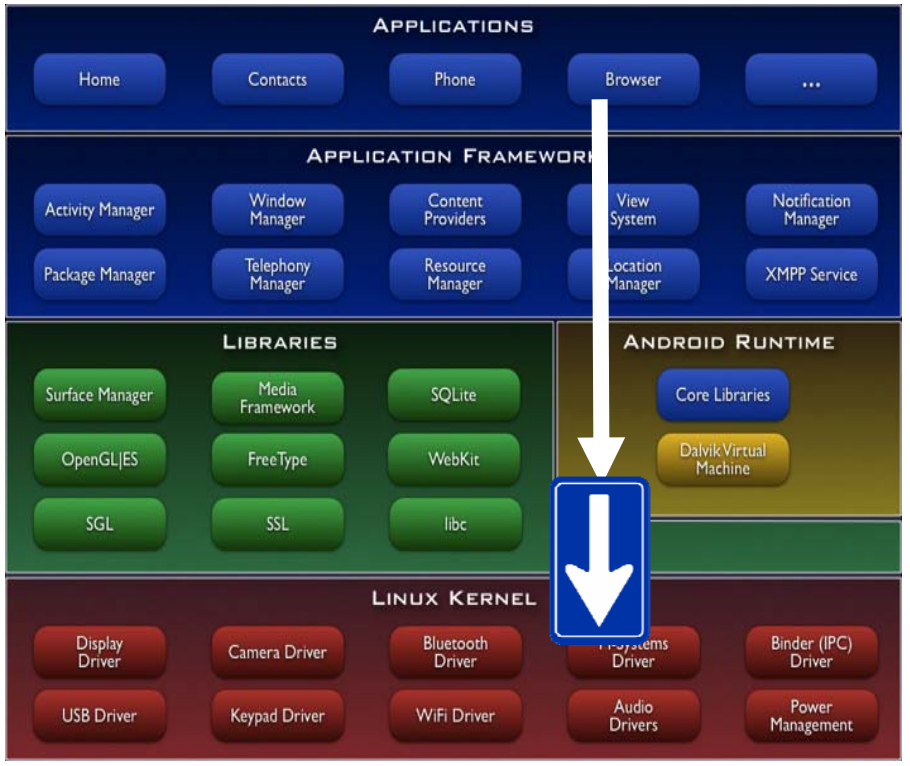
- 連携の必要性
  - 様々な技術分野、産学分野、法制度の連携による解決が必要。

Confidential
©2010 KDDI R&D Laboratories Inc.
KDDI R&D LABS

Androidの特徴

- OSの特徴
  - LinuxにDalvik仮想マシンを実装し、アプリをサンドボックス上で実行する。
  - アプリのインストールにはユーザ承認が必要であり、Windows XPのような自動感染型ウイルス・ワームの脅威は殆ど無い。
  - アプリのパーミッションを承認することで、ユーザがサンドボックスに穴を開ける。

ユーザの誤操作でマルウェアに感染



Confidential
©2010 KDDI R&D Laboratories Inc.
KDDI R&D LABS

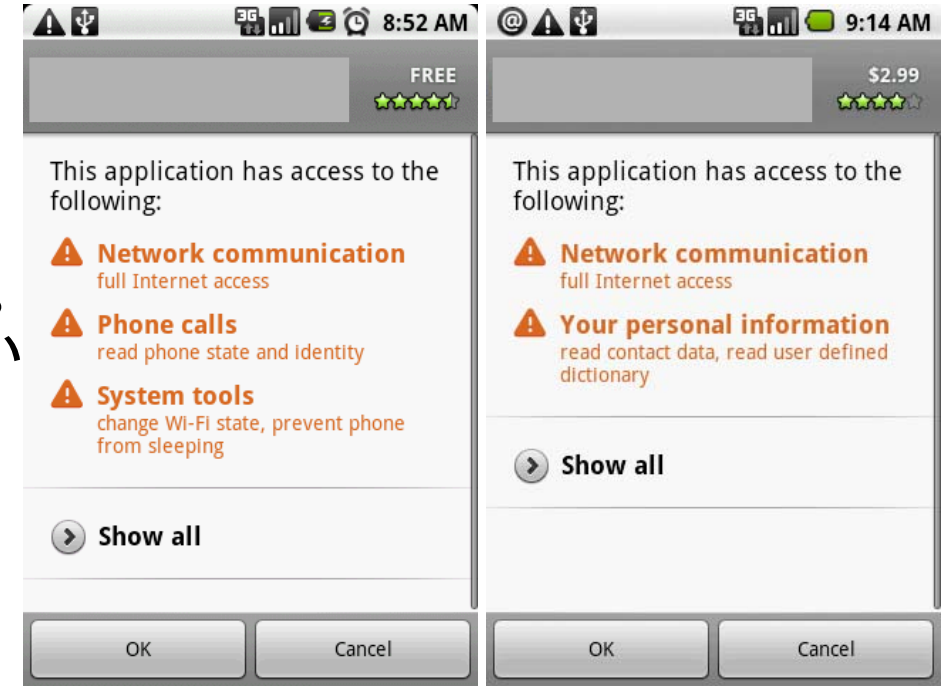
パーミッションによる承認

■ Dalvik VMの特徴
- ◆ ユーザは、アプリのパーミッション（潜在脅威）を閲覧してインストールを判断する。

■ パーミッションフレームワークの功罪

功 ユーザ承認で、個人情報や各種機能を利用する便利なアプリを実装できる。

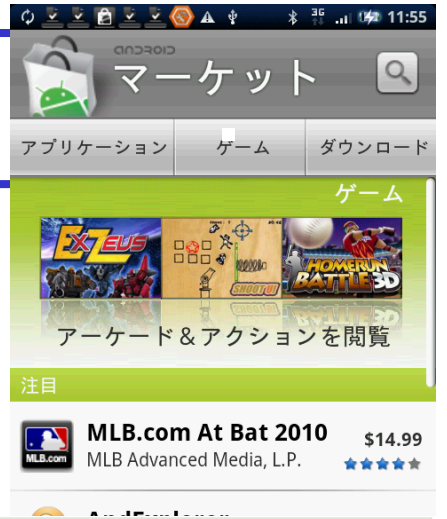
罪 パーミッションの潜在脅威を見抜けないユーザは、マルウェアに感染する。



■ パーミッションフレームワークの問題点
- ◆ 機能単位の利用申請であり、悪意の有無とは直接関連しない。
- ◆ そもそもパーミッションを気にするユーザは少ない…。

©2010 KDDI R&D Laboratories Inc.

Androidのマルウェア感染経路



- Androidの利点
  - 世界中の開発者がアプリを開発・公開している。
  - ユーザは、様々なアプリをインストールして高機能化を図る。

- Android Market上のアプリ(2010/9/26現在)
  - 13万以上のアプリが公開されている。
  - 16億ダウンロードを超えている。

- 問題点
  - Android Marketでは、無審査でアプリが公開されるため、マルウェアが混入する。

http://jp.androlib.com/appstats.aspx

©2010 KDDI R&D Laboratories Inc.

スパイウェアの一例

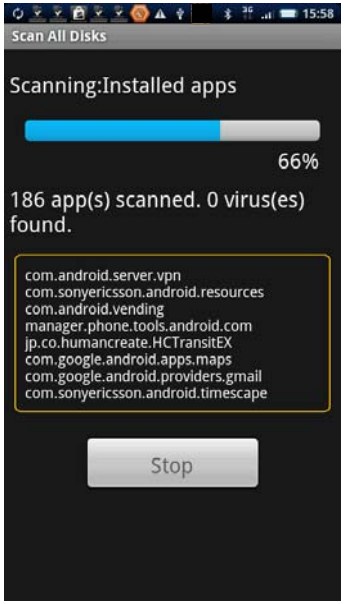
■ 表面上の機能

- ◆ 某ウイルス対策アプリは、インストールアプリをスキャンしてウイルスを検知する。
- ◆ 本物のウイルスは一つも検知できない。

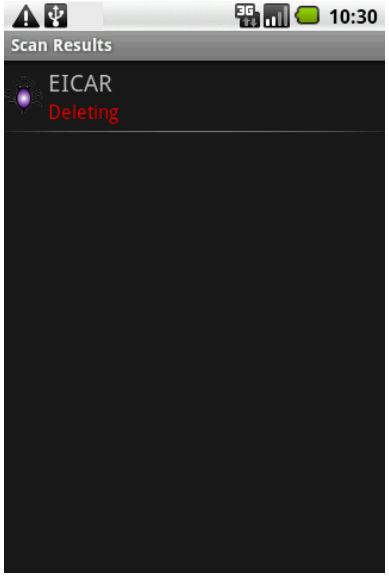
■ 31個のパーミッション
◆INTERNET、DELETE_PACKAGES、
RESTART_PACKAGES、READ_PHONE_STATE、
RECEIVE_SMS、READ_CONTACTS、WRITE_CONTACTS、
CALL_PHONE、READ_SMS、WRITE_SMS、SEND_SMS、
GET_TASKS、RECEIVE_BOOT_COMPLETED、
INSTALL_PACKAGES、ACCESS_NETWORK_STATE、
WRITE_APN_SETTINGS、PROCESS_OUTGOING_CALLS、
INSTALL_SHORTCUT、LOCATION、
ACCESS_FINE_LOCATION、
ACCESS_LOCATION_EXTRA_COMMANDS、
ACCESS_MOCK_LOCATION、
ACCESS_COARSE_LOCATION、
ACCESS_COARSE_UPDATES、CALL_PRIVILEGED、
MODIFY_PHONE_STATE、GOOGLE_AUTH.mail、
WAKE_LOCK、WRITE_EXTERNAL_STORAGE、
USE_CREDENTIALS、VIBRATE

パーミッション承認

スキャンの様子



本物のウイルスを非検知



■ 問題点

- ◆ アプリの挙動をモニタしたところ、ユーザの許可なく端末ID（IMEI）、契約 ID（IMSI）がアプリ作成者のサーバに送信された。

⇒ PCで起きていたトロイの木馬と同じことが発生している。

Confidential
©2010 KDDI R&D Laboratories Inc.
KDDI R&D LABS

アドウェアの一例

- 無料アプリの収入源
  - アプリに広告を掲載し、ユーザのクリックで開発者に報酬が入る。
- 仕組み
  - 国コード、緯度・経度を取得し、適切な言語で広告を表示する。
  - TEL番号、Android ID、IMEI、IMSI 、広告先を識別する。
- 問題
  - 広告事業者は、情報の利用目的をユーザに知らせることなく、自動的に収集している。
    （パーミッションによる承認で、情報収集の可能性はユーザに確認済み。）

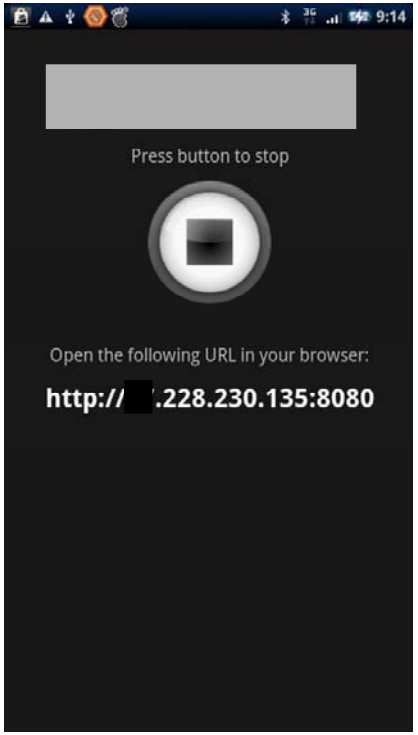
Confidential
©2010 KDDI R&D Laboratories I

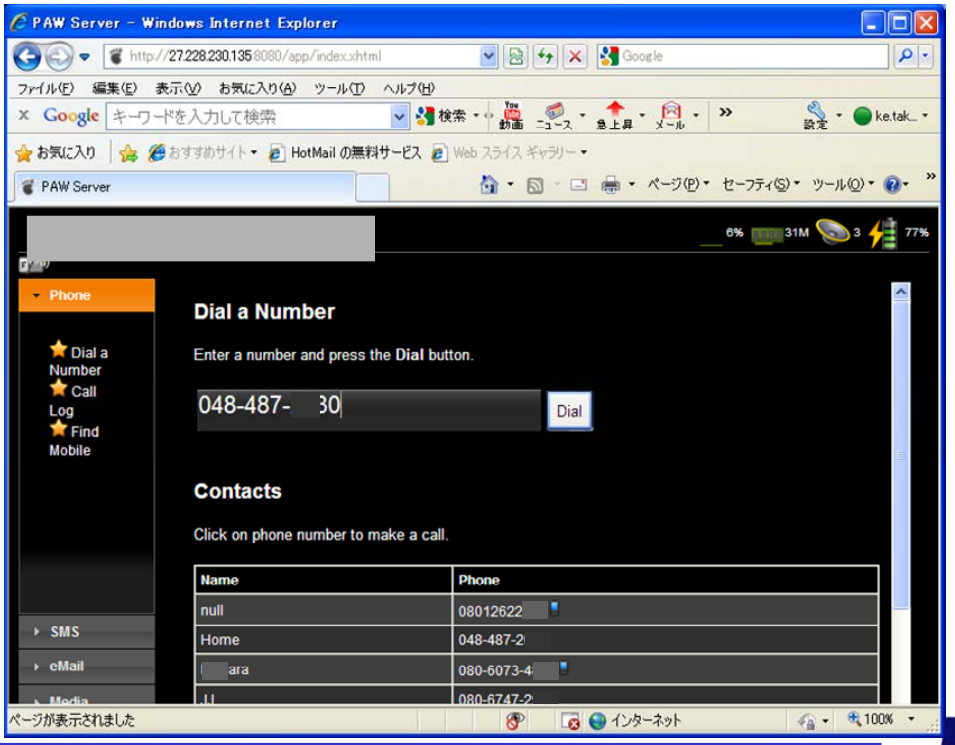
リモート制御アプリの一例

■ リモート制御アプリ
- ◆ Android端末を操作を、リモートPCからプッシュ型で制御する。

■ 懸念
- ◆ 踏み台アプリによる、Android端末のボットネット化が可能である。

グローバルIPを持つAndroid端末をリモート制御してTEL／メールさせるアプリ





Confidential
©2010 KDDI R&D Laboratories Inc.
KDDI R&D LABS

提言

■ 教育
- ◆ Androidは世界標準のOSが搭載されたPCである。

⇒ 一般ユーザ：アプリに潜在する脅威と自己責任モデルについての教育が必要。
⇒ アプリ開発者：利便性・広告収入に潜むアプリの踏み台化についての教育が必要。

■ 静的解析
- ◆ パーミッションの承認で、ユーザの自己責任にするには酷なのでは？！

⇒ Androidアプリの静的解析で、脅威を顕在化させて承認を求める仕組みが必要。

■ 法律
- ◆ Androidアプリは、逆コンパイルが容易なJava型アプリである。

⇒ コード解析による不正コピーアプリの氾濫に対する取り締まりが必要。
⇒ マルウェア検知の為なら、コード解析は正当行為としての整理すべき。

■ Trust Computing
- ◆ LinuxベースのOSであり、root権限奪取やチューニングが容易である。

⇒ 電波を発信する端末であり、改造させない保護技術が必要。

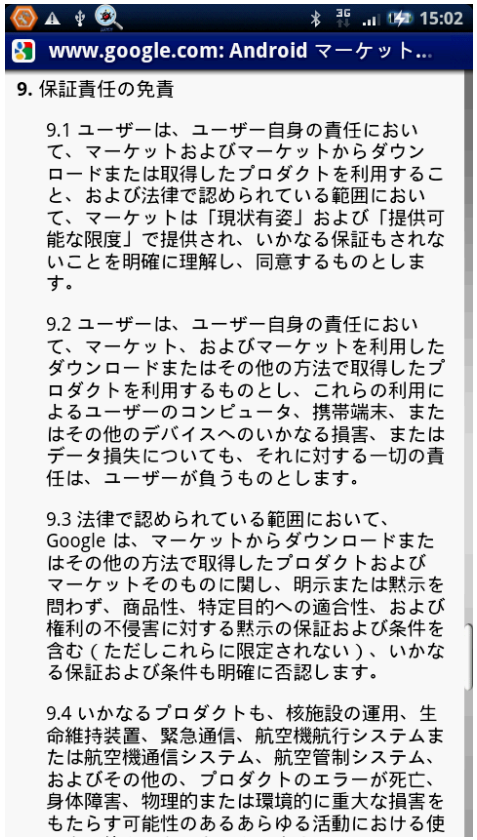
Confidential
©2010 KDDI R&D Laboratories Inc.
KDDI R&D LABS

付録：啓蒙活動への取り組み

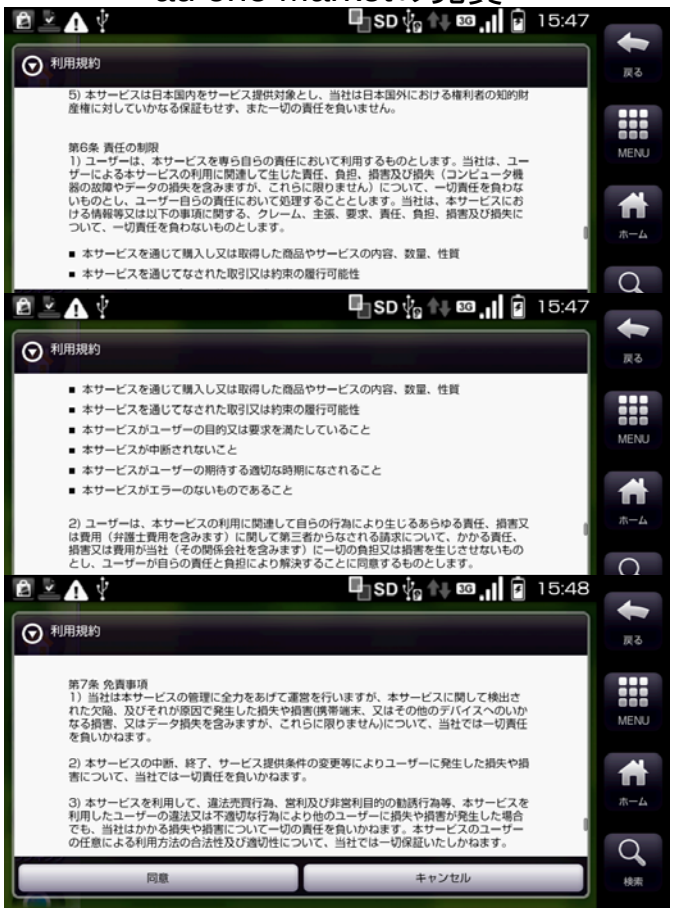
■ 利用規約を通じた啓蒙活動

- ◆ Market運用者は、ユーザ責任でアプリのDL・インストール・利用について注意喚起している。
- ◆ 通信事業者は、さらに踏み込んで端末の取扱説明書を通じて、Market利用の危険性と自己責任に関する啓蒙活動に努めている。

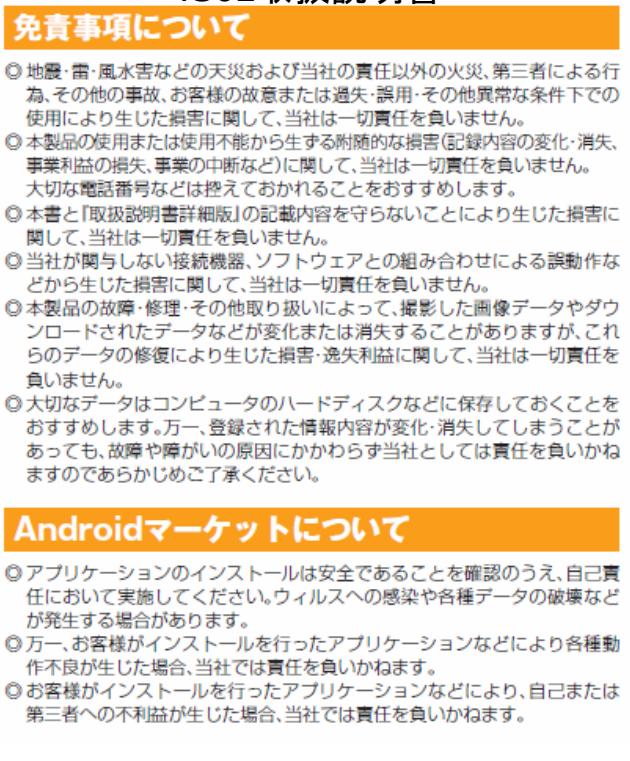
Android Marketの免責



au one Marketの免責



IS01取扱説明書



免責事項について

◎地震・雷・風水害などの天災および当社の責任以外の火災、第三者による行為、その他の事故、お客様の故意または過失・誤用・その他異常な条件下での使用により生じた損害に関して、当社は一切責任を負いません。
◎本製品の使用または使用不能から生ずる附随的な損害（記録内容の変化・消失、事業利益の損失、事業の中断など）に関して、当社は一切責任を負いません。大切な電話番号などは控えておかれることをおすすめします。
◎本書と「取扱説明書詳細版」の記載内容を守らないことにより生じた損害に関して、当社は一切責任を負いません。
◎当社が関与しない接続機器、ソフトウェアとの組み合わせによる誤動作などから生じた損害に関して、当社は一切責任を負いません。
◎本製品の故障・修理・その他取り扱いによって、撮影した画像データやダウンロードされたデータなどが変化または消失することがありますが、これらのデータの修復により生じた損害・逸失利益に関して、当社は一切責任を負いません。
◎大切なデータはコンピュータのハードディスクなどに保存しておくことをおすすめします。万一、登録された情報内容が変化・消失してしまうことがあっても、故障や障がいの原因にかかわらず当社としては責任を負いかねますのであらかじめご了承ください。

Androidマーケットについて

◎アプリケーションのインストールは安全であることを確認のうえ、自己責任において実施してください。ウィルスへの感染や各種データの破壊などが発生する場合があります。
◎万一、お客様がインストールを行ったアプリケーションなどにより各種動作不良が生じた場合、当社では責任を負いかねます。
◎お客様がインストールを行ったアプリケーションなどにより、自己または第三者への不利益が生じた場合、当社では責任を負いかねます。

Confidential
©2010 KDDI R&D Laboratories Inc.
KDDI R&D LABS

付録：マルウェア感染防止への取り組み

■ ユーザ向けの安全サービス

◆ au one Marketセキュアアプリ検証を受けたアプリに、安全マークを付与している。

■ アプリ開発者への啓蒙活動

◆ au one Marketセキュアアプリ検証で確認するポイントを明確にすることで、安全なアプリ開発を促している。

au one Marketセキュアアプリの検証では、以下の点に関する確認を実施しています。

1. 利用を宣言した機能（セキュリティー権限）の確認。
2. KDDIが提供しているAndroidアプリ配信サーバから配信していること。
3. KDDIから出荷されるAndroid端末の標準設定で利用できない機能の有無の確認。
4. 顧客情報を漏洩する動作、もしくは、漏洩する恐れのある動作の有無。
5. 不必要な大量通信の有無、もしくは、外部への不正アクセス機能の有無。

Confidential
©2010 KDDI R&D Laboratories Inc.
KDDI R&D LABS